Quiz 1
Coding Theory

20^{th} January 2006

Time: 1 hours (12:30–1:30pm)

1. Write the addition [3]† and multiplication [4] tables for $\mathbf{Z}_6$.

Solution. The addition table,

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

#

The multiplication table,

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

#

2. Given ISBN 0 19 8538□3 0. Find the missing digit □.[3]

Solution. For ISBN $x_1 \dots x_1 0$,

$$\sum_{i=1}^{10} i x_i \equiv (\mathrm{mod}\ 11)$$

Writing y for □,

$$0 + 1(2) + 9(3) + 8(4) + 5(5) + 3(6) + 8(7) + y(8) + 3(9) = 187 + 8y \equiv 0 (\mathrm{mod}\ 11)$$

Hence $y = 0$, and the ISBN is therefore 0 19 853803 0.

#

3. Let $f(x) = 1 + x^2 + x^3$. Show whether $f(x)$ is irreducible over $\mathbf{Z}_2$.[4] Then find $\mathbf{Z}_2[x]/\left(f(x)\right)$.[4] And then draw the addition [5] and multiplication [7] tables of $\mathbf{Z}_2[x]/\left(f(x)\right)$.

Solution. We note that $f(x)$ is of degree 3. Suppose $f(x)$ be reducible. Then it would have a linear factor x or $1 + x$, which would make 0 and 1 roots of $f(x)$. But $g(0) = g(1) = 1$, which is in $\mathbf{Z}_2$. Therefore $f(x)$ is irreducible.

#

$$\mathbf{Z}_2[x]/\left(1 + x^2 + x^3\right) = \left\{0, 1, x, 1 + x, x^2, x + x^2, 1 + x^2, 1 + x + x^2\right\}$$

#

† Numbers between square brackets are marks.

The addition table,

$+$	0	1	x	$1+x$	x^2	$x+x^2$	$1+x^2$	$1+x+x^2$
0	0	1	x	$1+x$	x^2	$x+x^2$	$1+x^2$	$1+x+x^2$
1	1	0	$1+x$	x	$1+x^2$	$1+x+x^2$	x^2	$x+x^2$
x	x	$1+x$	0	1	$x+x^2$	x^2	$1+x+x^2$	$1+x^2$
$1+x$	$1+x$	x	1	0	$1+x+x^2$	$1+x^2$	$x+x^2$	x^2
x^2	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$	0	x	1	$1+x$
$x+x^2$	$x+x^2$	$1+x+x^2$	x^2	$1+x^2$	x	0	$1+x$	1
$1+x^2$	$1+x^2$	x^2	$1+x+x^2$	$x+x^2$	1	$1+x$	0	x
$1+x+x^2$	$1+x+x^2$	$x+x^2$	$1+x^2$	x^2	$1+x$	1	x	0
								#

The multiplication table,

$\cdot$	0	1	x	$1+x$	x^2	$x+x^2$	$1+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x	$1+x$	x^2	$x+x^2$	$1+x^2$	$1+x+x^2$
x	0	x	x^2	$x+x^2$	$1+x^2$	1	$1+x+x^2$	$1+x$
$1+x$	0	$1+x$	$x+x^2$	$1+x^2$	1	$1+x+x^2$	x	x^2
x^2	0	x^2	$1+x^2$	1	$1+x+x^2$	x	$1+x$	$x+x^2$
$x+x^2$	0	$x+x^2$	1	$1+x+x^2$	x	$1+x$	x^2	$1+x^2$
$1+x^2$	0	$1+x^2$	$1+x+x^2$	x	$1+x$	x^2	$x+x^2$	1
$1+x+x^2$	0	$1+x+x^2$	$1+x$	x^2	$x+x^2$	$1+x^2$	1	$1+x$
								#